RAPID7 DATA SHEET

RAPID7 METASPLOIT EXPRESS

KEY BENEFITS

- Gain immediate insight into critical security threats in your IT infrastructure
- Save time and costs in remediation and notification costs by avoiding network downtime and/or averting a breach
- Leverage hundreds of fully tested and integrated exploit modules
- Create a heightened awareness of security's importance at the executive level
- Provide your security teams a strong basis for supporting approval of larger security budgets
- Determine if potential vulnerabilities represent real threats to your infrastructure without being burdened by a large number of false positives
- Simplify and accelerate your security testing program with an end-to-end penetration testing workflow via an easy-to-use graphical interface
- Meet regulatory compliance and prepare for security audits by implementing a formal security testing program
- Enhance your overall security by proactively eliminating identified security threats
- Detect common vulnerabilities that are outside of a normal audit scope, such as shared passwords across disparate systems

451 GROUP IMPACT BRIEF

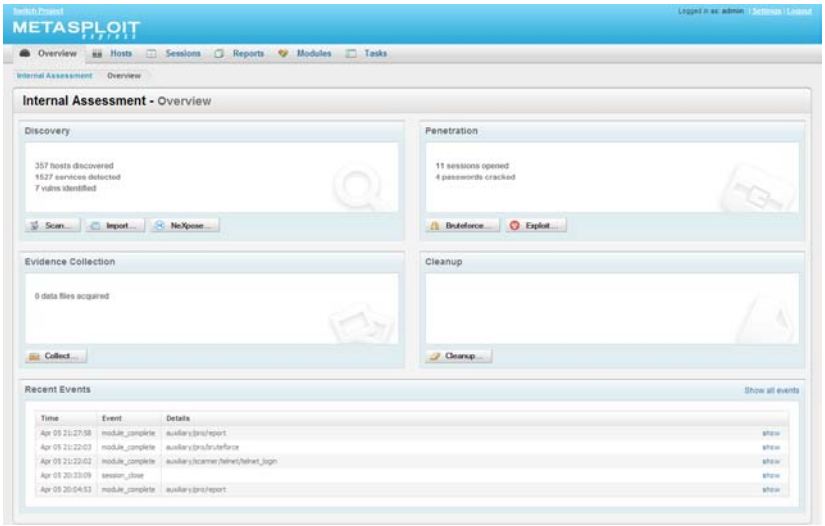
"Rapid7 is looking beyond compliance combining its Metasploit database of exploits with vulnerability data to give both security and operations a better understanding of risk."

the 451 group

METASPLOIT express

Organizations are struggling more than ever to identify the real risks to their data and infrastructure with the emergence of increasingly complex attack vectors. Penetration testing products have presented a viable mechanism to identify critical security threats, yet their complexity and cost have limited their use and deployment.

Metasploit Express was specifically designed for penetration testers and security professionals, addressing many of the key limitations of the existing market. Metasploit Express is an affordable, easy-to-use penetration testing solution that provides full network penetration testing capabilities, backed by the world's largest, fully tested and integrated public database of exploits. Metasploit Express not only automates exploits, but also detects and exploits common weaknesses such as simple passwords and insecure configurations.



Key characteristics:

- **Complete –** full network penetration testing capabilities with automated exploits; detects & exploits common weaknesses such as simple passwords and insecure configurations
- **Easy to use –** simple to use GUI interface supported by end-to-end workflow and reports
- **Safe –** test with confidence with exploit reliability rankings and the ability to throttle speed and concurrency as well as the option to only target safe exploits for risk prioritization
- **Integrated –** ships with pre-built integration with all versions of the market leading vulnerability management product Rapid7 NeXpose, Nmap and other solutions
- **Supported –** backed by Rapid7's customer support staff with dedicated SLAs for both Metasploit Express and supported components in the Metasploit Framework
- **Affordable –** available at a price point that a broad range of security professionals in large corporations, consulting organizations, and small business can leverage

RAPID7
UNIFIED VULNERABILITY MANAGEMENT

KEY PROCESS STEPS

- **Project Creation:**
  Initiate discrete internal and/or external components of a penetration test.
- **Discover Devices:**
  Identify hosts, scan for open ports and fingerprint the operating systems and services. Import scan data from NeXpose, Nmap and other solutions. NeXpose scans can also be initiated directly from within Metasploit Express.
- **Gain Access:**
  Gain access using Bruteforce, Exploitation and Manual Exploitation methods.
- **Take Control:**
  Create a command shell or Meterpreter session to control the device in the target environment.
- **Collect Evidence:**
  Gather artifacts for proof of access and obtain authentication credentials to go even deeper
- **Extend Access:**
  Recycle and replay capture authentication credentials to extend access to a greater number of targets
- **Cleanup and Reporting:**
  Close all open sessions and leverage a range of reports for viewing and exporting.

Automated Penetration Testing Workflow

Existing commercial products have been designed more as exploit execution platform and less as penetration testing solutions. Metasploit Express was created with the specific needs of a penetration tester in mind. The Metasploit Express Workflow Manager automates all penetration testing steps that security consultants would otherwise conduct manually, saving significant time, effort and expertise.

Leveraging the open source Metasploit Framework used by over 100,000 security professionals, Metasploit Express delivers the following core capabilities:

- **Latest Exploits and Payloads** – Leverages the world's largest, fully tested and integrated public database of exploits and payloads to conduct your tests.
- **Extensive Attack Targets** – Tests servers, desktops, Web servers, databases and devices. Automatically compromise database servers and network devices.
- **Full graphical user interface** – Simplifies usability and greatly enhances efficiency of penetration testers and security experts in a step-by-step model.
- **Robust live and configurable reports** – Ships with out-of-the box live, HTML, PDF and Word reports (executive summary report, detailed audit report, compromised hosts reports, collected evidence report, authentication tokens report). Export key findings via HTML and data files.
- **Powerful administration management** – Supports configurable administrative settings and site configurations and ships with standard and workflow XML-RPC interfaces.
- **Out-of-the box vulnerability management data integration** – Imports data from the market-leading vulnerability management solution NeXpose and other scanners or directly kick-off a NeXpose scan from within Metasploit Express to streamline tests.
- **Strong enterprise-class support offering** - Benefits from the support of the Metasploit community of over 100,000 users as well as guaranteed enterprise-level support with SLAs from Rapid7 customer care professionals.

ABOUT RAPID7

Rapid7 is the leading provider of unified vulnerability management, compliance, and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies.

Inc. 500

Deloitte. 2009 Technology Fast 500

DS 4/10

RAPID7

Feature Comparison: Version 3.4

		metasploit	METASPLOIT express
Core Features	Standard Metasploit Framework	✔	✔
	Latest Exploits and Payloads	✔	✔
	Automated Network Discovery	–	✔
	Smart Account Bruteforce	–	✔
	Smart Exploit Automation	–	✔
	Evidence Collection	–	✔
	Credential Recycling	–	✔
	Detailed Audit Logs	–	✔
Attack Configuration	Attack Browser	–	✔
Attack Targets	Servers, Desktops, Web Servers, Databases, Devices	✔	✔
	Automated Database Compromise	–	✔
	Automated Device Compromise	–	✔
Workflow	Penetration Testing Lifecycle Management Support (Discover, Gain Access, Take Control, Collect Evidence)	–	✔
	Targeting Workflow and Attack Iteration	–	✔
Report Options	Baseline 3rd Party Integration via XML	✔	✔
	Full Export Capabilities (XML + Data Files)	–	✔
	Standard Reports (Live Reports, PDFs, Word files)	–	✔
	Configurable Reports	–	✔
Usability & Administration	Command-Line Interface	✔	–
	Full Graphical User Interface (GUI)	–	✔
	Configurable Administrative Settings and Site Configurations	–	✔
	Out-of-the-Box NeXpose Integration	✔	✔
	Standard XML-RPC Interface	✔	✔
	Workflow XML-RPC Interface	–	✔
Support Options	Community-based Support	✔	✔
	Online Customer Support with Dedicated SLAs	–	✔
Installation & Configuration	Basic Installation	✔	–
	Advanced Installation & Configuration with full GUI	–	✔